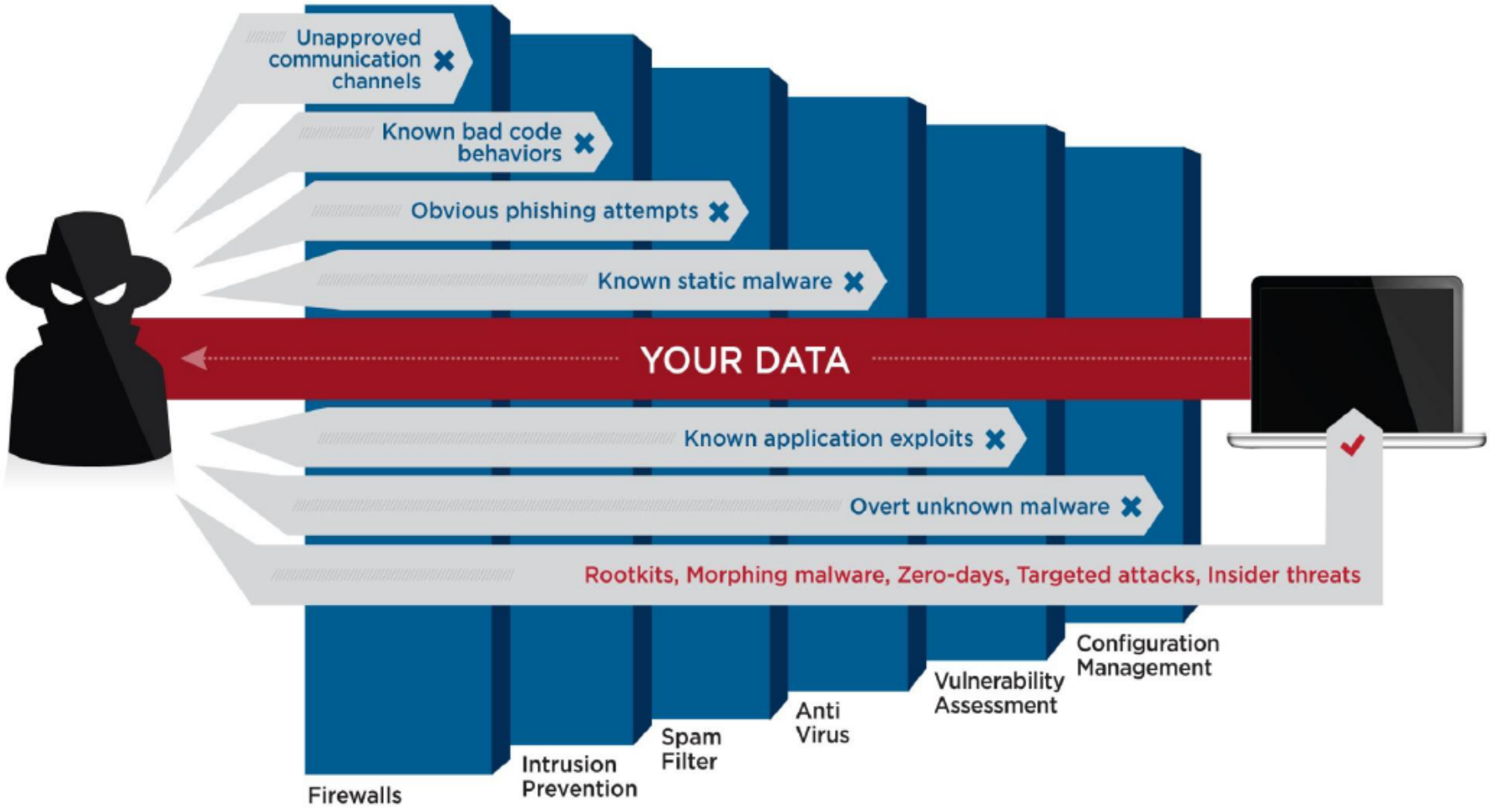
Big Data for Combating Cyber Attacks

Terry Janssen & Nancy Grady
Science Applications International Corp.

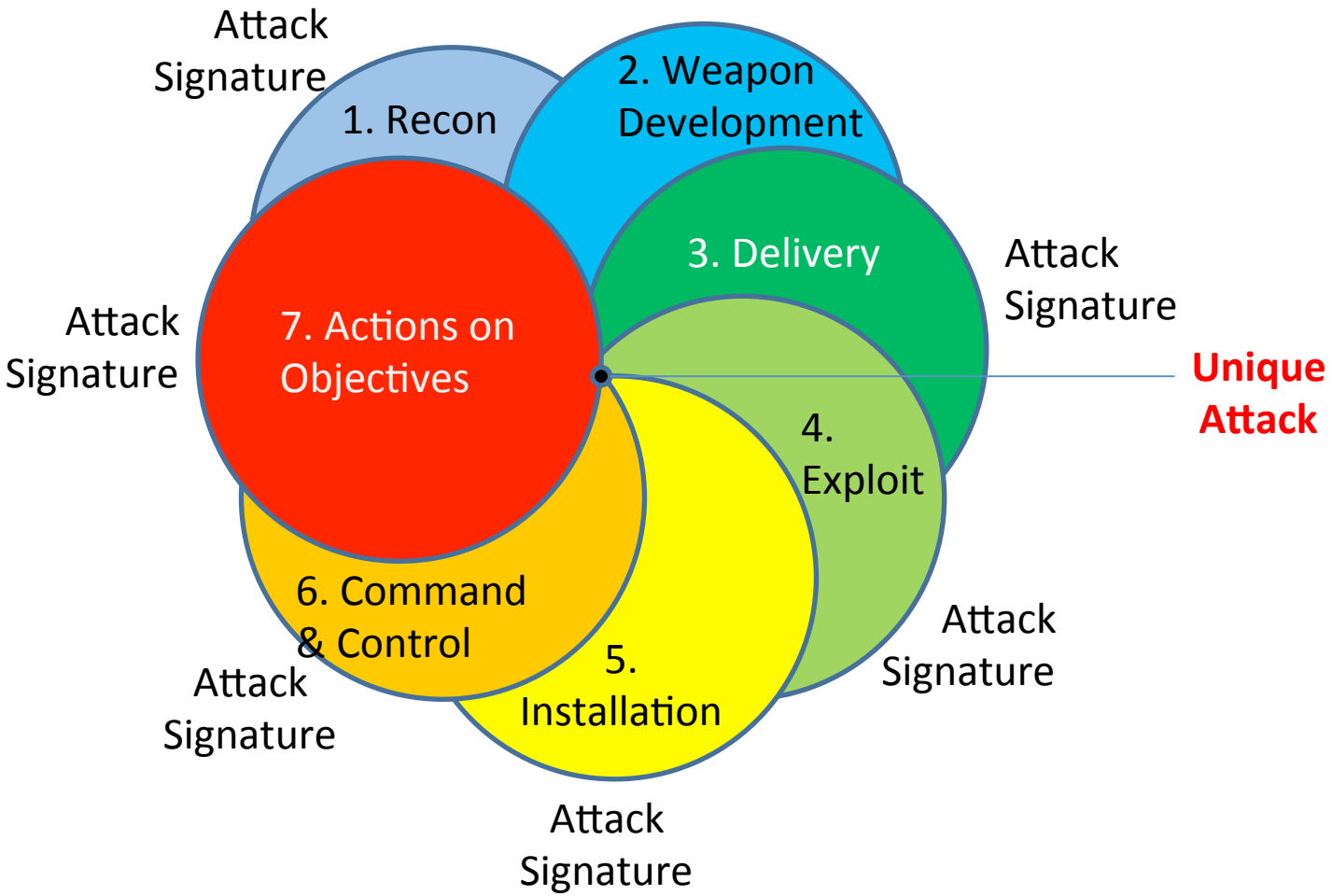
Cyber Attacks Penetrate The Best Architecture & Design



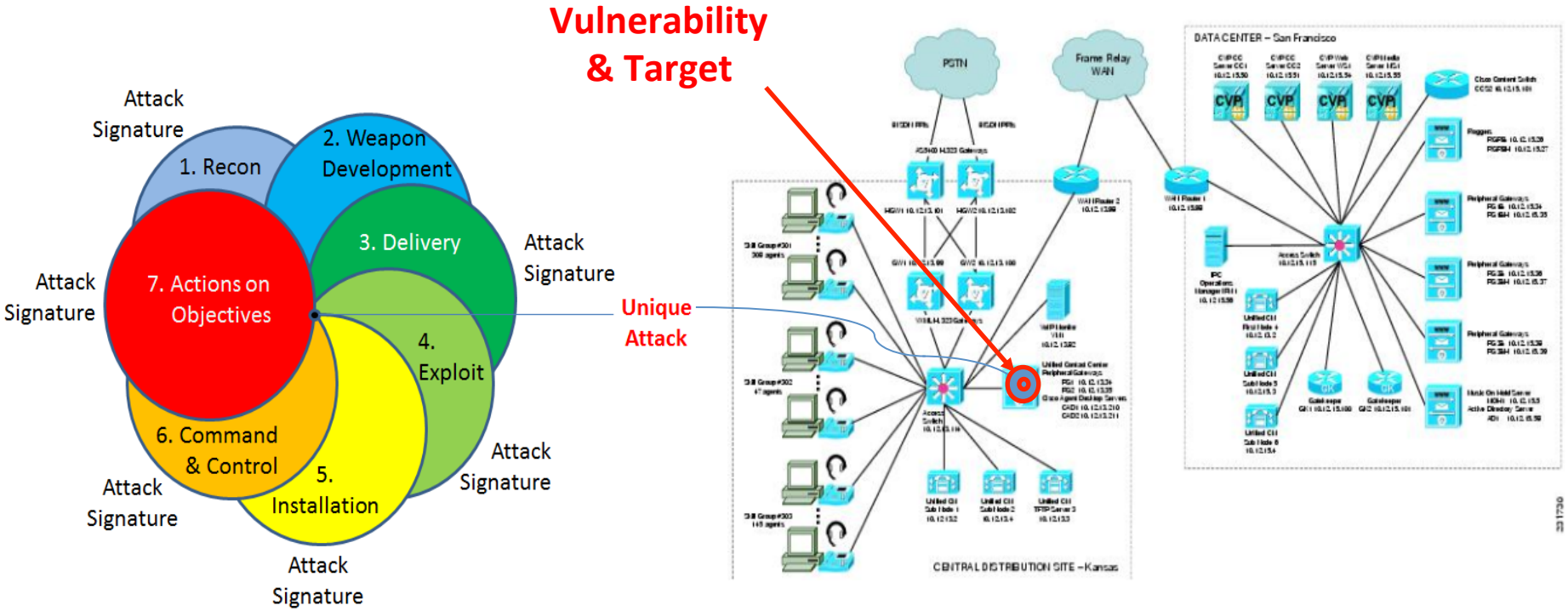
Why Big Data with Ontology?

- Today, “after-the-loss” scans/forensics are the status quo; losses are huge
- Cyber Big Data
  - Velocity, Volume, Variety & Veracity
- Exploration of Ontology
  - Cyber Big Data into knowledge structure
  - Foundation for Formal Methods like formal logic
  - Goal is Integration for SA & NRT Response

Correlation of Attack Signatures



Correlation of Attack with V & Target



Is Ontology with BD the Solution?

- Need **SA**, Just-in-Time **Reasoning** & NRT **Response**
  - Actionable data can decay in seconds; **manual too slow**
  - Loss prevention requires **NRT**
  - Big Data only provides the data, not the **knowledge structure and reasoning mechanism**

- **Surgically precise NRT responses** can prevent loss, e.g.,
  - Update Firewall immediately upon learning of a rogue IP Address or URL
  - Termination of a secure tunnel-out related to attacker